

UNITED STATES DISTRICT COURT

for the
Western District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)a) Microsoft account kjfox123@hotmail.com; b) Gmail accounts
irishclover4821@gmail.com and kevinjf83@gmail.com; c) Yahoo
accounts yankeeoutlaw55@yahoo.com and kevinfox102@yahoo.com;
and d) Verizon Wireless accounts 716-801-1256 and 585-307-0013

Case No. 16-M-1064

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York (identify the person or describe property to be searched and give its location): a) Microsoft account kjfox123@hotmail.com; b) Gmail accounts irishclover4821@gmail.com and kevinjf83@gmail.com; c) Yahoo accounts yankeeoutlaw55@yahoo.com and kevinfox102@yahoo.com; and d) Verizon Wireless accounts 716-801-1256 and 585-307-0013, which are more fully described in Attachments A1, A2, A3, and A4, respectively, which are attached hereto and incorporated by reference herein.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): Evidence pertaining to violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2), as more fully set forth in Attachments B1, B2, B3, and B4, respectively, which are attached hereto and incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2251(a), 2252A and 2261A(2), and the application is based on these facts: SEE AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

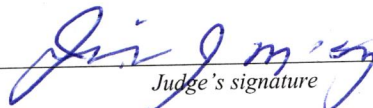

Applicant's signature

Brent S. Isaacson, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date:

8/1/16


Judge's signature

JEREMIAH J. MCCARTHY, U.S. Magistrate Judge
Printed name and title

City and state: Buffalo, New York

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brent S. Isaacson, being duly sworn, depose and say:

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed for nearly 20 years. I am assigned to the Jamestown Resident Agency of the FBI which is a part of the Buffalo Division of the FBI. In my career as an FBI Special Agent, I have investigated many federal crimes, including those involving the sexual exploitation of children. As a part of my official duties, I investigate violations of federal criminal law, including statutes which prohibit the production, distribution, and possession of child pornography, and cyberstalking.

2. I make this affidavit in support of an application for a search warrant, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and 18 United States Code §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to search the following items, where your affiant believes evidence exists of violations of Title 18, United States Code, Sections 2251(a) [production of child pornography], 2252A(a)(2)(A) [receipt of child pornography], 2252A(a)(5)(B) [possession of child pornography], and 2261A(2) [Cyberstalking]:

- a. Microsoft email account kjfox123@hotmail.com, located on the email servers of Microsoft Corporation located at 1065 La Avenida, Mountain View, CA 94043;
- b. Gmail email accounts irishclover4821@gmail.com and kevinjf83@gmail.com, located on the email servers of Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, CA 94043;

- c. Yahoo email accounts yankeeoutlaw55@yahoo.com and kevinfox102@yahoo.com, located on the email servers of Yahoo!, Inc., at 701 First Avenue, Sunnyvale, CA 94089; and
- d. Information associated with cell phone accounts 716-801-1256 and 585-307-0013, that is stored at premises controlled by Verizon Wireless;

hereinafter and collectively referred to as the "SUBJECT PROPERTY".

3. The information contained in this affidavit is based upon my personal participation in this investigation, information provided to me by other law enforcement officers involved in this investigation, and upon my training and experience. Because this affidavit is being submitted for the limited purpose of seeking search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2) exists on the SUBJECT PROPERTY.

I. INVESTIGATION AND FACTUAL BASIS

4. On June 23, 2016, an investigator of the Cattaraugus County Sheriff's Office ("CCSO") was contacted by a mental health professional who advised that a 48-year-old woman (whose identity is known to your affiant and who will hereinafter be referred to as "Adult Victim") had disclosed that she had been coerced into having and photographing sexual contact with her 17-year-old biological child (whose identity is known to your affiant and who will hereinafter be referred to as "Child Victim"). Adult Victim further disclosed that she had been receiving a large number of text messages on her cellular telephone which

appeared to originate from several different cellular telephone numbers. According to Adult Victim, the text messages made her believe that she, her boyfriend KEVIN JAMES FOX ("FOX"), and Child Victim were in danger of being assaulted by members of organized crime. Adult Victim was made to believe that the only way to avoid being targeted was for Adult Victim to engage in explicit sexual conduct with Child Victim and electronically send photographs of the conduct to the members of organized crime.

5. In response to this allegation, the CCSO interviewed Adult Victim and arranged for Child Victim to be interviewed at the Child Advocacy Center in Olean, New York. During the interview of Adult Victim, she stated that she has had a sexual relationship with FOX for about seven years. In recent weeks, Adult Victim has received hundreds of text messages from several different telephone numbers. These numerous text messages from many telephone numbers created a running text conversation among Adult Victim and several other personas that was accepted as genuine by Adult Victim. In sum and substance, Adult Victim came to believe that a woman named "Nicole" was an ex-girlfriend of FOX. "Nicole" discussed her desire to have group sexual encounters that included Nicole, Adult Victim, FOX, and other individuals. "Nicole," through many text messages, was persistent in requesting explicit sexual encounters with Adult Victim and others. The persistent requests for sexual conduct by "Nicole" became a nuisance to Adult Victim over time, and another person, "Robert," texted Adult Victim to ask whether Adult Victim wanted "Nicole" to cease contacting Adult Victim. Adult Victim said yes. Soon thereafter, FOX told Adult Victim via text message that "Nicole" had been badly beaten

and was in a coma. FOX asked Adult Victim whether she had asked for a "hit" on Nicole, and Adult Victim denied having asked for a "hit" on "Nicole." "Robert" in subsequent text messages to Adult Victim reinforced the notion that "Nicole" had been assaulted. Through numerous text messages from many different telephone numbers, Adult Victim came to believe that organized crime had assaulted "Nicole" based on a request by Adult Victim that "Nicole" cease making sexual requests via text. Adult Victim also came to believe that both she and FOX were now indebted to organized crime.

6. Adult Victim was told through many text messages from many telephone numbers that she was now in debt to organized crime. She was requested by the sender(s) of the text messages to repay the debt by having and photographing sexual encounters between Adult Victim and other men. As part of these demands, Adult Victim was forced to and did have sex with a two adult male neighbors, an African American adult male, and engaged in group sex activity with an adult male stranger and FOX. Some of these sexual encounters were photographed by Adult Victim and transmitted to FOX based on the demands by the organized crime personas. Adult Victim was ultimately told that she must repay the debt by having and photographing sexual conduct between Adult Victim and Child Victim. Adult Victim stated that she believed that she, Child Victim, and FOX were in grave danger from organized crime and that the only way to prevent harm coming to them was to acquiesce to the demands of the organized crime members.

7. As a result, Adult Victim told her child, Child Victim, about the danger posed

by the organized crime members and about their demands that she photograph sexual contact between her and Child Victim. According to Adult Victim, this generated a similar fear of the organized crime members in Child Victim's mind. On at least two occasions in June 2016, Adult Victim had sexual contact with Child Victim, and photographs of this sexual activity were transmitted electronically via text messages by Adult Victim to phone numbers Adult Victim believed belonged to members of organized crime.

8. Child Victim made disclosures during a videotaped interview at the Child Advocacy Center that were consistent with Adult Victim's disclosures to law enforcement. Child Victim corroborated the sexual contact with Adult Victim and the fear that Child Victim had toward the members of organized crime. Child Victim stated that on one occasion during which Child Victim and Adult Victim were engaging in explicit sexual conduct, Adult Victim was using the Skype application on a tablet computer to transmit live video of the sexual conduct to FOX. Child Victim could see on the tablet's screen that FOX was on the other end of the live video connection.

9. Adult Victim was hospitalized for several days for a mental health evaluation after making the above disclosures to law enforcement. Child Victim has been provided psychological trauma counseling by the Child Advocacy Center.

10. During interviews with law enforcement, Adult Victim gave her consent for law enforcement to search her cellular telephone and to assume her identity using her

telephone to communicate with FOX and others while posing as Adult Victim in an undercover capacity.

11. The CCSO and the FBI conducted forensic reviews of the cellular telephone used by Adult Victim. The data gleaned from Adult Victim's telephone closely corroborate the allegations made by Adult Victim. The review showed that Adult Victim received approximately 1,000 text messages from several different telephone numbers, most from area codes outside of the 716 area code where Adult Victim resides, from June 9, 2016, to June 22, 2016. The content of these text messages indicates that Adult Victim was being directed by the sender(s) of the texts to perform sexual acts with other adult men and also perform sexual acts with Child Victim. Adult Victim indicated that she was hopeful that acquiescing to the demands of producing images of her sexual contact with Child Victim would satisfy her debt to the organized crime members. The following is a text exchange on June 9, 2016, in which Adult Victim is told to produce images of sexual contact with Child Victim. Typographical, grammatical, and capitalization errors are included.

XXX-XXX-7185: Do not tell Kevin about this

XXX-XXX-7185: And you agree correct

Adult Victim: It has to be with two different guys or just one?

XXX-XXX-7185: You either have to do two guys tonight or pose for the pictures

Adult Victim: Two guys is going to be hard to do seeing I work til 1...

XXX-XXX-7185: You didn't answer about the two guys so now it's posing for the pictures

XXX-XXX-7185: Here is a list of pictures to send. his dick in your hand your tits in his. Your head between his legs and his between yours. You on top of him him on top of you both on your back and stomach. You bent over him behind you. Make sure they look real.

Adult Victim: Two guys would have been too hard to pull off tonight..even the pics are gonna be hard...

XXX-XXX-7185: I am just making you make it look real so do a good job of it

XXX-XXX-7185: But you both need to be naked so it looks real

Adult victim: I just hope I can find someone to get this done...I want all of this over with once and for all and so Kevin is safe as well...

XXX-XXX-7185: Understand

XXX-XXX-7185: What do you mean find

XXX-XXX-7185: This has to be done at home tonight

Adult Victim: With [Victim Child] you mean??!!!

XXX-XXX-7185: That's why I am going to let you two pose together

XXX-XXX-7185: You don't actually have to do the act just make it look like you are

Adult Victim: And then this is over with for good...nothing more...nothing held over my head anymore?

XXX-XXX-7185: Yes but it has to look real

Adult Victim: Alright

12. During the morning hours of June 10, 2016, Adult Victim sent several photographs via text message attachments to telephone number XXX-XXX-7185 depicting her and Child Victim engaging in oral and anal intercourse. I have reviewed these images

and have concluded that they constitute child pornography.

13. In the early morning hours of June 21, 2016, Adult Victim received text messages from a person utilizing telephone number XXX-XXX-1182 wherein she was directed to have sexual contact with Child Victim and send additional photographs to the unknown person. Adult Victim protested, stating "[Child Victim] told me something really sad...this really needs to be over with tonight and the best I'm going to be able to get him to do is for me to do the blowjob now ..he's not going to be able to do anything else." The person responded "then you two will do everything there is...fucking sucking and licking your pussy and fist you to...and then he is going to give you a shower." Adult Victim asked the person, "then it's over with right?" and the unknown person replied, "if you do everything." Adult Victim acknowledged her agreement to have the sexual contact with Child Victim and send images depicting the sexual contact to the unknown person.

14. A few hours later, Adult Victim sent several images to XXX-XXX-1182 which showed explicit sexual contact between Adult Victim and Child Victim. Included in these images were Adult Victim nude in a bath tub being urinated upon. Also depicted are photographs of oral sex between Adult Victim and Child Victim and a photograph that appears to be Child Victim's entire hand placed inside Adult Victim's vagina. I have reviewed these images and have concluded that they constitute child pornography.

15. Later in the day on June 21, 2016, Adult Victim received many text messages with two numbers, one belonging to FOX (XXX-XXX-0899) and one belonging to an

unknown person (XXX-XXX-1182). In sum and substance, the sender(s) of the texts originating from both telephone numbers indicated that Adult Victim should make and send additional pornographic images showing sexual contact between her and Child Victim. FOX stated, "No I don't understand why you are so beat up about it is all...big fucking deal you two had sex wow that is so painful." The unknown person using XXX-XXX-1182 stated, "line up at least two of your son's friends to join the two of you tonight. I don't care how you do it but it must be Skype." The Adult Victim protested, stating "I cannot do [Child Victim] again let alone his friends considering they are out of town have girlfriends and I'm not ruining another relationship again...and [Child Victim] cannot deal with this yet again and will not do it again...last night was the end of it for him."

16. On June 29, 2016, a law enforcement officer posed as Adult Victim by using her cellular telephone to have a text message conversation with FOX. During this exchange, FOX admitted that he created a ruse with the intent to coerce Adult Victim into having sexual contact with Child Victim, take photographs of the sexual contact, and send the photographs to FOX. FOX admitted that he created additional phone numbers and false personas to deceive Adult Victim into believing her and Child Victim were in danger from organized crime. FOX stated via text messages that he "made up everything there...there you have it...I'm the one who made you do all the terrible things...I am the one that you were talking to all the time...I am the one." FOX admitted that the persons with whom Adult Victim had communicated were, in fact, FOX posing as various people using different telephone numbers. FOX stated that he used his cellular telephone and a

technique which he described as "Star 811" to change the number of his cellular telephone as he was texting with Adult Victim. He also admitted that he had received the images depicting the sexual contact between Adult Victim and Child Victim and that no other people had received those images.

17. Adult Victim's cellular telephone was made in China. Included in Adult Victim's cellular telephone are text messages directing Adult Victim to send video to FOX's Skype address, kjfox123.

18. On July 1, 2016, Detective Sergeant Mark Crosson of the CCSO and I interviewed FOX at his place of employment, the Seneca Allegany Casino in Salamanca, New York. FOX was employed as a security official at the casino. The interview was non-custodial. Detective Sergeant Crosson and I asked FOX for some of his time and advised FOX that we would leave at the end of the conversation because we knew it was a busy night at the casino with Fourth of July events. FOX agreed to speak with Detective Crosson and me, and the conversation took place in FOX's supervisor's office in private.

19. FOX stated that the texts that were received by Adult Victim were "smoke and mirrors" and not true. In particular, he stated that he used three telephone applications or "apps" – TextFree, TextNow, and TextMe – which allowed FOX to create several telephone numbers from which he could send and receive texts from Adult Victim. He stated that by using multiple numbers, he was able to create the illusion in Adult Victim's

mind that she was now involved with the mob. FOX admitted that he used this ruse for the purpose of manipulating Adult Victim into performing and photographing sexual acts with Child Victim and then taking photographs of this sexual activity to send to FOX. FOX stated that his motives to do this were both for his sexual gratification and because he was angry with Adult Victim. FOX was angry with Adult Victim because she was unfaithful in her relationship with FOX.

20. FOX was shown hard copy prints of the child pornography images law enforcement discovered on Adult Victim's cellular telephone. FOX stated that he recognized these child pornography images as those he received from Adult Victim as a result of pressuring Adult Victim with the ruse about the mob. While he was reviewing the images, FOX made handwritten notations on the hard copy prints of the images to indicate which photographs included Adult Victim engaged in sexual contact with Child Victim.

21. FOX stated that at the time he pressured Adult Victim into having sexual contact with Child Victim, FOX knew that Child Victim had recently reached his 17th birthday.

22. During the course of the interview, Detective Sergeant Crosson and I asked FOX whether he would be willing to complete a written statement to summarize the information he provided. He agreed to do so. The text of this statement follows, verbatim:

Time: July 1, 2016

7:00 p.m.

I, Kevin James Fox, Sr., wish to provide the following voluntary statement to Detective Sergeant Mark Crosson and FBI Special Agent Brent S. Isaacson. I understand that I am not under arrest. I am giving this statement freely, and no promises or threats have been made to me.

I have had an 8 year long relationship with [Adult Victim]. In approximately mid April, [Adult Victim] and I had a falling out of sorts. I became angry with [Adult Victim] at some point. I decided to create a fictitious (sic) story about the mob. To do so, I created several phone numbers, I posed as various people including Robert, Mary, Cheryl, Kristen, and Nicole. I wrote text messages to [Adult Victim] to make her believe she was now involved with the mob. I pressured her to have various types of sexual relationships. In recent weeks, I pressure her to have sexual contact with her son, [Child Victim]. I knew that [Child Victim] had just turned 17 year old. I suggested certain sexual act be performed between [Adult Victim] and [Child Victim]. [Adult Victim] and [Child Victim] did perform those sexual acts. At my direction, [Adult Victim] transmitted photographs of sexual acts between her and [Child Victim] to my cell phone and iPad. I received those images. At this interview, I was shown hard copy photographs. These are some of the images I received from [Adult Victim]. I made handwritten notations on these hardcopy photographs to identify the males in the pictures. Some of these pictures included [Child Victim]. The only devices I used are the cell phone and the iPad. I factory reset these devices before today. I never shared these images with anyone else. The accounts I used to create cell phone numbers and through which I communicated with [Adult Victim] and received these images have been deleted by me before today. I did this to make sure the images would not be further distributed. The cell phone apps I used are Textfree, Textnow, and Textme.

I feel great regret for doing this. I will never do it again.

I have been given an opportunity to review this statement and make any changes I wish. This statement is true and accurate. I gave this statement voluntarily, and I have not been threatened or promised anything. The detective and agent have been friendly and professional with me today. This statement is 3 pages long.

//Kevin J. Fox//

//Mark Crosson//

//Brent S. Isaacson//

23. At the conclusion of the interview, the investigators shook FOX's hand, thanked him for his time, and departed the property of the Seneca Allegany Casino.

24. During an interview of Adult Victim, she disclosed it was in approximately 2014 that she first received a text from an unknown number, and that it was in February of 2016, that the text messages started to take an aggressive tone. During the interview, in addition to providing details about the sexual activity with her son, Adult Victim also stated that she had sexual contact with a 16 year old male at the direction of the organized crime personas. Adult Victim stated that at the direction of FOX, an advertisement seeking a young male sexual partner for Adult Victim was placed onto the Craigslist.com website. A 16 year old male responded to the advertisement, stating at first that he was 18 years old. He then disclosed that he was 16 years old. According to Adult Victim, when she told the organized crime personas that the respondent to the advertisement was only 16 years old, she was directed by the organized crime personas to have sexual contact with the 16 year

old male, photograph this sexual contact, and send the images to the organized crime personas via text message attachments, which she did. During the investigation, law enforcement found photographs depicting Adult Victim and a young male on Adult Victim's cellular telephone. According to Adult Victim, contraband images of sexual contact between Adult Victim and this minor were sent to organized crime personas via text message attachments.

25. Adult Victim told law enforcement that Craigslist.com advertisements placed by FOX or by Adult Victim at FOX's direction were associated with two email accounts, yankeeoutlaw55@yahoo.com and irishclover4821@gmail.com, which were utilized by FOX and Adult Victim, respectively. According to Adult Victim, FOX knew the login information, including passwords, for both email accounts. Because of their connection to the illegal production of child pornography, it is requested that a search of these emails be granted by the Court.

26. A forensic review of the Adult Victim's cellular telephone and an interview of Adult Victim revealed several email accounts that were either utilized by FOX or for which FOX had login information including passwords. Further, as a part of the organized crime ruse that FOX used to extort Adult Victim to send illegal child pornography images to FOX, FOX directed that Adult Victim use the website Craigslist.com to advertise for male sexual partners. Text messages exchanged among Adult Victim and the organized crime personas controlled by FOX showed that they shared email addresses and their

corresponding login and password information. Adult Victim stated that this was for the purpose of allowing FOX to monitor responses from advertisements on Craigslist.com seeking sexual partners. The organized crime personas created by FOX also directed that Adult Victim transmit to FOX live video, via the Internet application "Skype," of her sexual contact with Child Victim. The text messages between Adult Victim and the organized crime personas showed that FOX's Skype account name was kjfox123.

27. According to an interview of Child Victim, during one episode of sexual contact with Adult Victim, Adult Victim attempted to utilize a tablet computer running the Skype application to transmit live video of the sexual contact to FOX. Child Victim saw FOX on the tablet computer on the other end of the video connection. Child Victim refused to engage in sexual activity while Skype was running, and subsequently threw the tablet.

28. As alleged by Adult Victim and as admitted by FOX, illegal child pornography digital images were sent to FOX by Adult Victim by text messaging. The receipt, storage, and transmission of digital image files is made very easy with today's personal computers and communications devices, and it is reasonable to conclude that the illegal images received by FOX could have been stored in email accounts for later retrieval and distribution. Once FOX came into possession of the illegal child pornography images, it would be a straightforward process for him to conceal, store, or transmit the images by using email accounts under his control or for which he had login information.

29. According to Adult Victim, FOX also utilized email address kjfox123@hotmail.com. This is consistent with the records of the Microsoft, Incorporated, which maintains the Skype video conferencing service. Microsoft records revealed that the email addresses kjfox123@hotmail.com and kevinfox102@yahoo.com were associated with Skype account names found in the Adult Victim's cellular telephone. Microsoft records and a review of Adult Victim's cellular telephone revealed that Adult Victim also had a Skype account with an associated email address of irishclover4821@gmail.com.

30. According to the records of Pinger, Incorporated, the company which operates the TextFree text messaging application, two phone numbers which texted Adult Victim's cellular telephone as a part of FOX's organized crime ruse were associated with the email addresses kevinfox102@yahoo.com, kevinjf83@gmail.com, and yankeeoutlaw55@yahoo.com.

31. According to Adult Victim and consistent with a review of her cellular telephone, Adult Victim's cellular telephone number was 716-801-1256 and FOX's cellular telephone number was 585-307-0013. Both numbers were operated by Verizon Wireless from January 1, 2016 until at least June of 2016. This Court's authority is requested to search the records of Verizon Wireless for data, including subscriber information, call detail records, SMS data records and cellular tower and cell site sector (cell site locations) information, Per Call Measurement Data (PCMD) information, and any and all data

connections related to the use of telephone numbers 716-801-1256 and 585-307-0013, that will assist law enforcement in corroborating the violations of federal child pornography statutes alleged herein.

II. TECHNICAL BACKGROUND

A. Microsoft

32. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Microsoft allows subscribers to obtain e-mail accounts at the domain name "hotmail.com" like the e-mail account used by FOX. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Hotmail subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, e-mail transaction information, and account application information.

33. In general, an e-mail that is sent to a Microsoft subscriber is stored in the subscriber's "in-box" on Microsoft servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Microsoft and other ISPs have provided their users with larger

storage capabilities associated with the user's e-mail account. Currently, Microsoft now provides users up to 15 gigabytes of free storage space using Microsoft's storage platform known as OneDrive (formerly known as SkyDrive).

34. OneDrive, and its relic SkyDrive, is a file hosting, storage, and sharing service that is provided by Microsoft for Microsoft Hotmail account users. Microsoft OneDrive/SkyDrive has been integrated into Microsoft Hotmail and is linked to, associated with, and accessible using a Hotmail e-mail account. The integration allows users to directly upload documents and photos within Hotmail, store them on OneDrive/SkyDrive, and share with other users.

35. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Microsoft's servers, and then transmitted to its end destination. Microsoft often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Microsoft server, the e-mail can remain on the system indefinitely.

36. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail.

37. A Microsoft subscriber can also store files, including e-mails, address books,

contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Microsoft.

38. Subscribers to Microsoft might not store on their home computers copies of the e-mails stored in their internet based accounts. This is particularly true when they access their account through smartphones or the web, or if they do not wish to maintain particular e-mails or files in their residence.

39. In general, e-mail providers like Hotmail ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

40. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account) and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because

every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

41. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

42. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

B. Google

43. Similar to Microsoft, Google offers a free email service to users known as Gmail, which allows subscribers to obtain an email address at the domain name "gmail.com". In addition to sending and receiving email through Gmail, Google users have access to various Google services that can be used to store various types of data such as Google Picasa, Google+, Google Earth, Google Docs, Google Calendar, Google Voice, Google Drive, Google Blogger, and Google Hangouts.

44. I have been informed by other agents that Google's policies prohibit mailing or emailing child pornography to law enforcement in response to a search warrant; instead requiring a law enforcement officer to personally appear and collect contraband materials, unless the means of production is explicitly described in that search warrant. Google has shared with law enforcement the following sample language which, if included in a search warrant, will enable Google to delivery child pornography material via mail without violating its internal policies: "Google shall disclose responsive data, if any, by sending to [street address] using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code." Therefore, as part of the warrant attachment for the Gmail accounts including in this application, the language provided by Google will be included.

C. Yahoo

45. Similar to Microsoft and Google, Yahoo offers a free email service to users which allows subscribers to obtain an email address at the domain name "yahoo.com".

D. Verizon Wireless

46. In my training and experience, I have learned that Verizon Wireless is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for Verizon Wireless subscribers may be located on the computers of Verizon Wireless.

47. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of Verizon Wireless for weeks or months.

48. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by Verizon Wireless for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

49. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or

multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

50. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

51. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which "cell towers" (i.e., antenna towers covering specific geographic areas) received

a radio signal from the cellular device and thereby transmitted or received the communication in question.

52. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

53. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

54. Since FOX and Adult Victim both utilized Verizon Wireless cellular telephones, information stored at Verizon Wireless, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such "timeline" information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device's owner

and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

III. CONCLUSION

55. Based upon the above information, I believe that probable cause exists to believe there has been a violation of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2), and that there is probable cause to believe that on:

- a. Microsoft email account kjfox123@hotmail.com, located on the email servers of Microsoft Corporation located at 1065 La Avenida, Mountain View, CA 94043, which is more fully described in **Attachment A1**;
- b. Gmail email accounts irishclover4821@gmail.com and kevinjf83@gmail.com, located on the email servers of Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, which is more fully described in **Attachment A2**;
- c. Yahoo email accounts yankeeoutlaw55@yahoo.com and kevinfox102@yahoo.com, located on the email servers of Yahoo!, Inc., at 701 First Avenue, Sunnyvale, CA 94089, which is more fully described in **Attachment A3**; and
- d. Information associated with cell phone accounts 716-801-1256 and 585-307-0013, that is stored at premises controlled by Verizon Wireless, which is more fully described in **Attachment A4**;

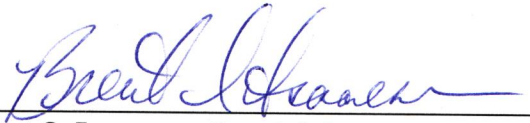
there are located those items set out in **Attachments B1, B2, B3, and B4**, respectively.

56. In consideration of the foregoing, I respectfully request that this Court issue a search warrant for the property known as:

- a. Microsoft email account kjfox123@hotmail.com, located on the email servers of Microsoft Corporation located at 1065 La Avenida, Mountain View, CA 94043, which is more fully described in **Attachment A1**;
- b. Gmail email accounts irishclover4821@gmail.com and kevinjf83@gmail.com, located on the email servers of Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, which is more fully described in **Attachment A2**;
- c. Yahoo email accounts yankeeoutlaw55@yahoo.com and kevinfox102@yahoo.com, located on the email servers of Yahoo!, Inc., at 701 First Avenue, Sunnyvale, CA 94089, which is more fully described in **Attachment A3**; and
- d. Information associated with cell phone accounts 716-801-1256 and 585-307-0013, that is stored at premises controlled by Verizon Wireless, which is more fully described in **Attachment A4**;

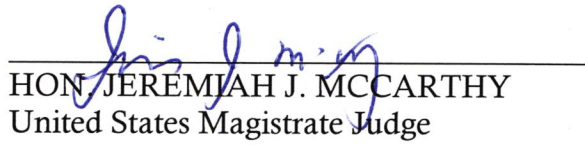
authorizing the search of the aforementioned property for the items described in **Attachments B1, B2, B3, and B4**, respectively.

57. Finally, since this affidavit relates to an ongoing criminal investigation and contains email addresses and/or other identifying information of the individuals who are witnesses and/or targets in this matter, the government respectfully moves this Court to issue an Order sealing, for 60 days unless the Court orders otherwise, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the required inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the premises to be searched).



Brent S. Isaacson, Special Agent
Federal Bureau of Investigation

Sworn to before me this 1st day of
August, 2016



HON. JEREMIAH J. MCCARTHY
United States Magistrate Judge

ATTACHMENT A1
DESCRIPTION OF PROPERTY TO BE SEARCHED

Microsoft email account kjfox123@hotmail.com, located on the e-mail servers of Microsoft Corporation located at 1065 La Avenida, Mountain View, CA 94043.

ATTACHMENT A2
DESCRIPTION OF PROPERTY TO BE SEARCHED

Gmail email accounts irishclover4821@gmail.com and kevinjf83@gmail.com, located on the email servers of Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT A3
DESCRIPTION OF PROPERTY TO BE SEARCHED

Yahoo email accounts yankeeoutlaw55@yahoo.com and kevinfox102@yahoo.com, located on the email servers of Yahoo!, Inc., at 701 First Avenue, Sunnyvale, CA 94089.

ATTACHMENT A4
DESCRIPTION OF PROPERTY TO BE SEARCHED

Information associated with cell phone accounts 716-801-1256 and 585-307-0013, that is stored at premises owned, maintained, controlled, or operated by Verizon Wireless, a wireless provider headquartered at 180 Washington Valley Road, Bedminster, NJ 07921.

ATTACHMENT B1
LIST OF ITEMS TO BE SEIZED

I. Schedule of Items to be Disclosed by Microsoft

To the extent that the information described in **Attachment A1** is within the possession, custody, or control of Microsoft, Microsoft is required to disclose the following information to the government for the account or identifier listed in **Attachment A1**. Such information should include the below-described content of the subject account:

- a. The contents of all e-mails and instant messages stored in the account, including copies of e-mails and instant messages sent to and from the account, the source and destination addresses associated with each e-mail and/or instant message, the date and time at which each e-mail/instant message was sent, and the size and length of each e-mail/instant message;
- b. Any deleted e-mails or instant messages, including any information described in subparagraph "a," above;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. All records or other information stored by an individual using the account, including profile, address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between Microsoft and any person regarding the account, including contacts with support services and records of actions taken.
- f. All records, content, and subscriber information, of the OneDrive/SkyDrive account associated with kjfox123@hotmail.com.

II. Schedule of Items to be Searched for and Seized by the Government

For the period of time from January 1, 2014, to the present, and from the items listed in Section I, any and all evidence relating to violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2), that pertains to the following:

- a. The production, receipt, distribution, or possession of child or adult pornography, and any attempted activity to do so.
- b. Solicitations to engage in sexual activity.
- c. Postings on craigslist.com or any other internet bulletin board.
- d. Threats of violence or physical harm.
- e. Text messaging applications.
- f. Communications mentioning or from "Robert," "Mary," "Cheryl," "Kristen," "Nicole" or any other organized crime persona.
- g. Communications regarding organized crime.
- h. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner.
- i. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

ATTACHMENT B2
LIST OF ITEMS TO BE SEIZED

I. Schedule of Items to be Disclosed by Google

To the extent that the information described in **Attachment A2** is within the possession, custody, or control of Google, Google is required to disclose the following information to the government for the account or identifier listed in **Attachment A2**. Such information should include the below-described content of the subject account:

- a. The contents of all e-mails and instant messages stored in the account, including copies of e-mails and instant messages sent to and from the account, the source and destination addresses associated with each e-mail and/or instant message, the date and time at which each e-mail/instant message was sent, and the size and length of each e-mail/instant message;
- b. Any deleted e-mails or instant messages, including any information described in subparagraph "a," above;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. All records or other information stored by an individual using the account, including profile, address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.
- f. All records, content, and subscriber information relating to Google Picasa, Google+, Google Earth, Google Docs, Google Calendar, Google Voice, Google Drive, Google Blogger, and Google Hangouts.

Google shall disclose responsive data, if any, by sending to the U.S. Attorney's Office, ATTN: Aaron J. Mango, 138 Delaware Avenue, Buffalo, New York, 14202, using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.

II. Schedule of Items to be Searched for and Seized by the Government

For the period of time from January 1, 2014, to the present, and from the items listed in Section I, any and all evidence relating to violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2), that pertains to the following:

- a. The production, receipt, distribution, or possession of child or adult pornography, and any attempted activity to do so.
- b. Solicitations to engage in sexual activity.
- c. Postings on craigslist.com or any other internet bulletin board.
- d. Threats of violence or physical harm.
- e. Text messaging applications.
- f. Communications mentioning or from "Robert," "Mary," "Cheryl," "Kristen," "Nicole" or any other organized crime persona.
- g. Communications regarding organized crime.
- h. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner.
- i. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

ATTACHMENT B3
LIST OF ITEMS TO BE SEIZED

I. Schedule of Items to be Disclosed by Yahoo

To the extent that the information described in **Attachment A3** is within the possession, custody, or control of Microsoft, Microsoft is required to disclose the following information to the government for the account or identifier listed in **Attachment A3**. Such information should include the below-described content of the subject account:

- a. The contents of all e-mails and instant messages stored in the account, including copies of e-mails and instant messages sent to and from the account, the source and destination addresses associated with each e-mail and/or instant message, the date and time at which each e-mail/instant message was sent, and the size and length of each e-mail/instant message;
- b. Any deleted e-mails or instant messages, including any information described in subparagraph "a," above;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- d. All records or other information stored by an individual using the account, including profile, address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between Yahoo and any person regarding the account, including contacts with support services and records of actions taken.

II. Schedule of Items to be Searched for and Seized by the Government

For the period of time from January 1, 2014, to the present, and from the items listed in Section I, any and all evidence relating to violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2), that pertains to the following:

- a. The production, receipt, distribution, or possession of child or adult pornography, and any attempt to do so.

- b. Solicitations to engage in sexual activity.
- c. Postings on craigslist.com or any other internet bulletin board.
- d. Threats of violence or physical harm.
- e. Text messaging applications.
- f. Communications mentioning or from "Robert," "Mary," "Cheryl," "Kristen," "Nicole" or any other organized crime persona.
- g. Communications regarding organized crime.
- h. Communications regarding the physical location of targets, subjects, or victims of the investigation.
- i. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner.
- j. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

ATTACHMENT B4
LIST OF ITEMS TO BE SEIZED

I. Schedule of Items to be Disclosed by Verizon Wireless

To the extent that the information described in **Attachment A4** is within the possession, custody, or control of Verizon Wireless, including any messages, records, files, logs, or information that have been deleted but are still available to Verizon Wireless or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Verizon Wireless is required to disclose the following information to the government for each account or identifier listed in **Attachment A4**:

- a. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from January 1, 2014, to present;
- d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message;
- e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;
- f. Detailed billing records, showing all billable calls including outgoing digits, from January 1, 2014, to present;
- g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from January 1, 2014 to present;
- h. Incoming and outgoing telephone numbers, from January 1, 2014, to present;

- i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;
- j. All records pertaining to communications between Verizon Wireless and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Schedule of Items to be Searched for and Seized by the Government

For the period of time from January 1, 2014, to the present, and from the items listed in Section I, any and all evidence relating to violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2261A(2), that pertains to the following:

- a. The production, receipt, distribution, or possession of child or adult pornography, and any attempted activity to do so.
- b. Solicitations to engage in sexual activity.
- c. Postings on craigslist.com or any other internet bulletin board.
- d. Threats of violence or physical harm.
- e. Text messaging applications.
- f. Communications mentioning or from "Robert," "Mary," "Cheryl," "Kristen," "Nicole" or any other organized crime persona.
- g. Communications regarding organized crime.
- h. Communications regarding the physical location of targets, subjects, or victims of the investigation.
- i. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crimes under investigation.
- j. Evidence indicating the geographic location of the cellular device at times relevant to the investigation.
- k. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).

1. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to the production, receipt, distribution, or possession of child or adult pornography, including records that help reveal their whereabouts.